

# Physical Layer Security in MIMO Backscatter Wireless Systems

Qian Yang, *Student Member, IEEE*, Hui-Ming Wang, *Senior Member, IEEE*,  
Yi Zhang, *Student Member, IEEE*, and Zhu Han, *Fellow, IEEE*

**Abstract**—Backscatter wireless communication is an emerging technique widely used in low-cost and low-power wireless systems, especially in passive radio frequency identification (RFID) systems. Recently, the requirement of high data rates, data reliability, and security drives the development of RFID systems, which motivates our investigation on the physical layer security of a multiple-input multiple-output (MIMO) RFID system. In this paper, we propose a noise-injection precoding strategy to safeguard the system security with the resource-constrained nature of the backscatter system taken into consideration. We first consider a multi-antenna RFID tag case and investigate the secrecy rate maximization (SRM) problem by jointly optimizing the energy supply power and the precoding matrix of the injected artificial noise at the RFID reader. We exploit the alternating optimization method and the sequential parametric convex approximation method, respectively, to tackle the non-convex SRM problem and show an interesting fact that the two methods are actually equivalent for our SRM problem with the convergence of a Karush-Kuhn-Tucker (KKT) point. To facilitate the practical implementation for resource-constrained RFID devices, we propose a fast algorithm based on projected gradient. We also consider a single-antenna RFID tag case and develop a low-complexity algorithm which yields the global optimal solution. Simulation results show the superiority of our proposed algorithms in terms of the secrecy rate and computational complexity.

**Index Terms**—MIMO backscatter wireless communication, RFID, physical layer security, artificial noise, optimization.

## I. INTRODUCTION

**B**ACKSCATTER wireless communication, remarkable for its low energy consumption and low product cost, is an emerging technology which is widely used [1]–[4]. One of its most prominent applications is in radio frequency identification (RFID) systems. RFID enables identification from a distance, thereby facilitating the handling of manufactured goods and materials [1], [2]. By employing backscatter modulation [3] to send back the data and on-tag power harvesting [4] to supply the power, RFID is promoted by its longevity, efficacy,

and energy efficiency. It is believed that RFID will become one of the most crucial techniques to realize the Internet of Things (IoT) [5], which allows objects to be sensed and creates more efficient interactions between the physical world and computer-based systems.

As a contactless technology in a short range, RFID systems are expected to fulfill the aim of reducing handling time despite the augment of data stored in RFID tags [6], [7]. Concerning this higher expectation of the data rate and data reliability for novel RFID applications, the implementation of the multiple-input multiple-output (MIMO) scheme appears to be effective and promising [8], [9], which attracts considerable research interests [10]–[14]. It is shown in [10] that adopting multiple antennas can extend the coverage of backscatter RFID systems and improve system capacity under the spatial multiplexing configuration. Furthermore, the authors in [11], [12] show that multi-antenna techniques can significantly improve the data reliability of the RFID system. The space-time coding scheme is explored in [13], [14] for MIMO RFID backscatter systems. Apart from the above analytical studies, several real experiments concerning multi-antenna RFID tags have also been conducted [15]–[17]. The measurement results in [15] show that read range can be improved when multiple antennas, instead of a single antenna, are equipped at the RFID tag. In addition, the authors in [16] propose a method for channel measurements in MIMO RFID systems. The authors in [17] showcase two multi-antenna techniques for RFID tags operating at 5.8 GHz. The MIMO scheme has been extensively investigated and recognized as an efficient approach to further extending the information-carrying ability of RFID [9].

Due to the widespread deployment of RFID tags, the privacy concern for users, such as clandestine physical tracking and personal information protecting, also makes a great challenge to the design of RFID systems, because the transmission is vulnerable to eavesdropping due to the broadcast nature of backscatter communication [18]–[20]. Most of previous works concerning RFID security issues mainly focus on lightweight cryptography such as in [20]–[22]. However, they still have some restrictions on the secret key generation and distribution from eavesdropping and practical limitations in terms of size, cost, and computation [22], [23]. Fortunately, in recent years physical layer security (PLS), as an alternative or complement to cryptography, has drawn considerable attention in strengthening the security of wireless communications since perfect secrecy is provided. The theoretical basis for PLS approaches lies in the notion of the *secrecy capacity/rate*, which was pioneered by Wyner in [24]. Since then, wealth

The work of Q. Yang, H.-M. Wang, and Y. Zhang was partially supported by the National Natural Science Foundation of China under Grant 61671364, the Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant 201340, and the Young Talent Support Fund of Science and Technology of Shaanxi Province under Grant 2015KJXX-01. The work of Z. Han was supported in part by the U.S. NSF ECCS-1547201, CCF-1456921, CNS-1443917, ECCS-1405121, and NSFC 61428101. (*Corresponding author: Hui-Ming Wang.*)

Q. Yang, H.-M. Wang, and Y. Zhang are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: yangq36@gmail.com; xjbswhm@gmail.com; yi.zhang.cn@outlook.com).

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA (e-mail: zhan2@uh.edu).

of relevant research has achieved a significant success in the security of conventional wireless communication systems [25]–[32]. The main idea of PLS approaches, in addition to exploiting the randomness inherent to wireless channels [27], is to manually construct *equivalent channels* via signal design and power allocation such that the superiority of the equivalent legitimate channel to the equivalent wiretap channel can be established [33]. One of promising approaches is to send an artificially generated noise to deteriorate the channel condition of eavesdroppers. This conception of applying artificial noise (AN) to enhance the secure transmission is first introduced in [28], and it is further studied in [29]–[32]. These studies have also been generalized to the cooperative relay system [33]–[36].

However, there is only little work to study the security of backscatter systems from the perspective of PLS. In [23], a physical layer noise injection scheme is proposed to strengthen the security of backscatter wireless systems under a single-input single-output (SISO) system setting where all terminals employ a single antenna, and it is shown that the proposed approach yields significant performance gains. To the best of our knowledge, no work has been done on the PLS of a MIMO backscatter system, even though the MIMO technique is promising in enhancing the security due to extra spatial degrees of freedom provided by multiple antennas [29]. Note that the PLS approaches for the conventional MIMO system cannot be directly used into the MIMO backscatter system due to the following two reasons. For one thing, the channel model of the MIMO backscatter system is quite different from the conventional one and usually is modeled as the so-called *dyadic backscatter channel* [4], which makes it hard to formulate the considered security problem. For another thing, the passive backscatter system is typically resource-constrained and thus requires low-complexity algorithms in practice. Particularly, the trade-off between secrecy performance and computational complexity should be taken into account in the algorithm design of the MIMO backscatter system.

Based on the above observations, in this paper we focus on solving the security issues of a MIMO RFID system from the perspective of PLS, wherein we take full account of the resource-constrained nature of RFID devices. The novelty and main contributions of this paper can be summarized as follows:

- 1) The MIMO backscatter wireless communication is studied from the perspective of PLS for the first time and a noise-injection precoding strategy is proposed to strengthen the security of the system.
- 2) The *alternating optimization* (AO) method and the *sequential parametric convex approximation* (SPCA) method are, respectively, invoked to tackle the non-convex *secrecy rate maximization* (SRM) problem. Furthermore, we show an interesting fact that the two methods are actually equivalent for our problem.
- 3) Particularly, a custom-designed algorithm based on *projected gradient* (PG) is proposed for fast implementation, which is especially beneficial to the resource-constrained RFID device.
- 4) As a complement, the case where the tag has only a single

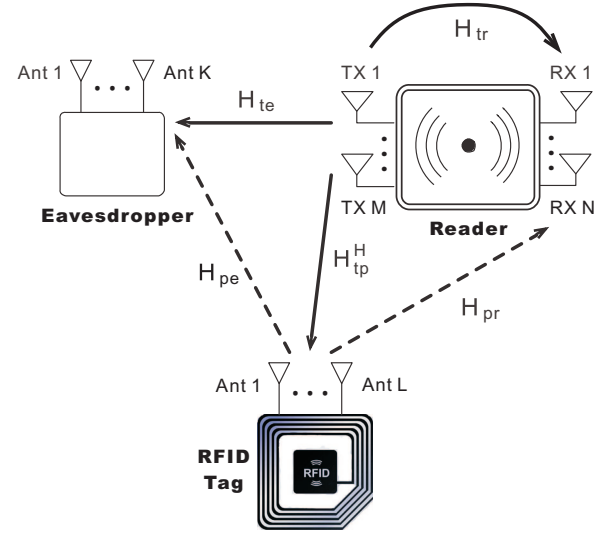


Fig. 1. The MIMO backscatter system, consisting of a RFID reader, a RFID tag, and a passive eavesdropper.

antenna is studied, and the global optimal solution can be obtained by one-dimensional search. Moreover, a nullspace AN design in this case is further proposed, and it is shown in the simulations that this scheme obtains the secrecy rate which is close to the optimal one and enjoys an extremely low computational complexity.

The rest of this paper is organized as follows: In Section II, we present the system model and develop the formulation for the achievable secrecy rate of a MIMO RFID backscatter system. In Section III, we focus on the SRM problem with a multi-antenna tag, and the equivalence of the AO and SPCA methods is analyzed. In Section IV, we propose a fast algorithm to efficiently solve the SRM problem with a multi-antenna tag. The case where the tag equips with only a single antenna is studied in Section V. Numerical simulations and analysis for the proposed schemes and algorithms are presented in Section VI before the conclusions drawn in Section VII.

**Notations:**  $\mathbf{A}^T$ ,  $\mathbf{A}^H$ ,  $\det(\mathbf{A})$  and  $\text{Tr}(\mathbf{A})$  represent the transpose, Hermitian transpose, determinant and trace of a matrix  $\mathbf{A}$ , respectively.  $\mathbf{I}$  denotes an identity matrix.  $\mathbf{A} \succeq \mathbf{0}$  means that  $\mathbf{A}$  is a Hermitian positive semidefinite matrix.  $\mathbb{E}\{\cdot\}$  and  $(\cdot)^*$  denote the expectation and conjugate, respectively.  $\mathbf{y} = [\mathbf{x}]^+$  means that  $y_i = \max\{0, x_i\}$  for every  $i$ .  $\text{diag}\{\mathbf{x}\}$  denotes a diagonal matrix with diagonal elements taken from vector  $\mathbf{x}$ .  $\mathbf{e}_i$  denotes a column vector whose the  $i$ -th element is 1 and 0 elsewhere.  $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$  means that  $\mathbf{x}$  is a random vector following a complex circular Gaussian distribution with mean  $\boldsymbol{\mu}$  and covariance  $\boldsymbol{\Sigma}$ .  $\circ$  represents the Hadamard product.

## II. SECURE MIMO BACKSCATTER SYSTEM MODEL

Consider a RFID system consisting of a multi-antenna RFID reader with  $M$  transmitting antennas and  $N$  receiving antennas, a RFID tag with  $L$  antennas, and a passive eavesdropper with  $K$  receiving antennas as shown in Fig. 1. For notational simplicity, we use the terms “reader” and “tag” as commonly used in RFID systems hereinafter.

The basic idea of realizing the RFID backscatter wireless communication is as follows: First, the reader transmits a continuous carrier wave (CW) to power up the tag. Then, the passive tag reflects back the CW signal by changing the different impedance loads of its antennas according to its stored secret information such as identification data. This procedure can be regarded as a backscatter modulation, where the secret information, to be transmitted from the tag to the reader, is modulated on the reflected CW signal by the tag. Finally, the reader extracts the desired information by estimating and decoding the echoed back signal after the backscatter modulation. During the whole backscatter procedure, the reader continuously transmits a CW signal to power up the tag and concurrently receives the echoed back signal modulated by the tag, namely, it works in a full-duplex mode. Thus, the received self-interference or leaked signal directly from its transmitter to receiver needs to be canceled. Whereas in practice, it is difficult for the reader to perform this cancellation without any signal leakage. Thereby in this work, we use  $\beta \in [0, 1]$  as in [37] to denote the self-interference attenuation factor which reflects the capacity for the reader to cancel the interference from the transmitted signal in the received signal. Based on the procedure above, under the assumption that all the channels undergo slow frequency-flat fading, the received signal at the reader is given by<sup>1</sup>

$$\mathbf{y}_r = \mathbf{H}_{pr} \mathbf{Q} \mathbf{H}_{tp}^H \mathbf{x} + \sqrt{\beta} \mathbf{H}_{tr} \mathbf{x}' + \mathbf{n}_r, \quad (1)$$

where  $\mathbf{x} \in \mathbb{C}^{M \times 1}$  is the signal transmitted by the reader<sup>2</sup> with the total power constraint  $\text{Tr}(\mathbb{E}\{\mathbf{x}\mathbf{x}^H\}) \leq P$ .  $\mathbf{H}_{tp}^H \in \mathbb{C}^{L \times M}$ ,  $\mathbf{H}_{pr} \in \mathbb{C}^{N \times L}$ , and  $\mathbf{H}_{tr} \in \mathbb{C}^{N \times M}$  represent the channel from the reader to the tag, the channel from the tag to the reader, and the self-interference channel at the reader, respectively.  $\mathbf{n}_r \sim \mathcal{CN}(\mathbf{0}, \sigma_r^2 \mathbf{I})$  is the additive white Gaussian noise (AWGN) at the reader.  $\mathbf{Q} \in \mathbb{C}^{L \times L}$  is the tag's information signaling matrix which represents the backscatter gain at the tag. The structure of  $\mathbf{Q}$  describes the backscatter modulation by the tag, during which the RF tag absorbs and scatters radio signals by its  $L$  antennas. This signaling matrix takes several different forms depending upon the physical implementation of the modulation circuitry and RF tag antennas [11]. In this paper, we consider a common scenario employed in [4], [10] that the signaling matrix  $\mathbf{Q}$  takes the form of a diagonal matrix, given by

$$\mathbf{Q} = \text{diag}\{q_1, q_2, \dots, q_L\} = \text{diag}\{\mathbf{q}\}. \quad (2)$$

We assume that the elements in vector  $\mathbf{q}$  are i.i.d. and  $\mathbb{E}\{\mathbf{q}\mathbf{q}^H\} = \mathbf{I}$ .

In this paper, we propose a noise-injection precoding scheme to create additional interference at the eavesdropper

<sup>1</sup>This signal model is first proposed in [10], wherein self-interference is not considered and only spatial domain is involved. The model in [10] is further generalized to the space-time coding model in [4], [13], [14] where temporal domain is also taken into account. In this paper, we focus on transmit optimization against eavesdropping only in spatial domain and thus adopt the signal model similar as that in [10].

<sup>2</sup>Since the reader receives its transmitted signals from both the backscatter and its self-interference channels at different time instants, we adopt  $\mathbf{x}'$  in (1) to denote the signal received directly from the reader's self-interference channel and distinguish it from the signal received from the backscatter channel, i.e.,  $\mathbf{x}$ . A similar notation will be also used in (6).

and thus to strengthen the security of the system. The transmit vector  $\mathbf{x}$  takes the structure  $\mathbf{x} = \mathbf{s} + \mathbf{z}$ , where  $\mathbf{s} \in \mathbb{C}^{M \times 1}$  is the CW signal to provide the tag with the power supply and we consider the conventional case as in uniform query<sup>3</sup> that the reader transmits a constant CW with the transmit power equally allocated among all its transmit antennas, i.e.,  $\mathbf{s} = \sqrt{P_s/M} \mathbf{1}_M$ , where  $P_s$  denotes the power allocated to the CW signal.  $\mathbf{z} \in \mathbb{C}^{M \times 1}$  is an AN vector, generated by the reader and injected into the transmitted CW signal, to interfere with the eavesdropper. Let  $\mathbf{\Lambda}_z \triangleq \mathbb{E}\{\mathbf{z}\mathbf{z}^H\} \succeq \mathbf{0}$  denote the spatial covariance matrix of the AN. The total power constraint at the reader now changes to

$$P_s + \text{Tr}(\mathbf{\Lambda}_z) \leq P. \quad (3)$$

For the considered MIMO RFID channel, the reader uses the noisy observation of  $\mathbf{H}_{pr} \mathbf{Q} \mathbf{H}_{tp}^H \mathbf{x}$  to estimate the unknown signal  $\mathbf{q}$  with the CW signal  $\mathbf{s}$ . We can rewrite  $\mathbf{H}_{pr} \mathbf{Q} \mathbf{H}_{tp}^H \mathbf{x}$  as

$$\begin{aligned} \mathbf{H}_{pr} \mathbf{Q} \mathbf{H}_{tp}^H \mathbf{x} &= \mathbf{H}_{pr} \text{diag}\{\mathbf{H}_{tp}^H \mathbf{x}\} \mathbf{q} \\ &= \sqrt{P_s} \mathbf{H}_{pr} \text{diag}\{\sqrt{1/M} \mathbf{H}_{tp}^H \mathbf{1}_M\} \mathbf{q} \\ &\quad + \mathbf{H}_{pr} \text{diag}\{\mathbf{H}_{tp}^H \mathbf{z}\} \mathbf{q}. \end{aligned} \quad (4)$$

For notational simplification, let  $\mathbf{D}_{tp} \triangleq \text{diag}\{\sqrt{1/M} \mathbf{H}_{tp}^H \mathbf{1}_M\}$  and  $\mathbf{F}_{tp} \triangleq \text{diag}\{\mathbf{H}_{tp}^H \mathbf{z}\}$ . We can rewrite (1) as

$$\mathbf{y}_r = \sqrt{P_s} \mathbf{H}_{pr} \mathbf{D}_{tp} \mathbf{q} + \sqrt{\alpha} \mathbf{H}_{pr} \mathbf{F}_{tp} \mathbf{q} + \sqrt{\beta} \mathbf{H}_{tr} \mathbf{z}' + \mathbf{n}_r, \quad (5)$$

where  $\alpha \in [0, 1]$ , following from the setting in [23], is the attenuation factor which denotes how successful the reader is in canceling the backscattered AN. Note that the CW signal  $\mathbf{s}'$ , received directly from the self-interference channel  $\mathbf{H}_{tr}$  at the reader, has been removed from (5) due to the fact that the standardized CW signal is commonly known and can be eliminated by the reader.

Similar to the reader, the received signal at the eavesdropper is given as

$$\mathbf{y}_e = \sqrt{P_s} \mathbf{H}_{pe} \mathbf{D}_{tp} \mathbf{q} + \mathbf{H}_{pe} \mathbf{F}_{tp} \mathbf{q} + \mathbf{H}_{te} \mathbf{z}'' + \mathbf{n}_e, \quad (6)$$

where  $\mathbf{H}_{pe} \in \mathbb{C}^{K \times L}$  and  $\mathbf{H}_{te} \in \mathbb{C}^{K \times M}$  are the tag-eavesdropper and reader-eavesdropper channel matrices, respectively.  $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_e^2 \mathbf{I})$  is the AWGN at the eavesdropper.  $\mathbf{H}_{pe} \mathbf{F}_{tp} \mathbf{q}$  is the backscattered AN signal modulated by the tag's information signal, while  $\mathbf{H}_{te} \mathbf{z}''$  is the injected noise term received directly from the reader-eavesdropper channel. It should be noted that, unlike the reader, the eavesdropper cannot perform AN attenuation due to the absence of the prior knowledge about the random AN signal  $\mathbf{z}$  transmitted by the reader. However, the CW signal received directly from the reader-eavesdropper channel can be eliminated by the eavesdropper due to the fact that the standardized CW signal is commonly known [23]. That is why this signal term does not appear in (6).

<sup>3</sup>There exist two different query methods widely adopted in the existing literature: the conventional uniform query [4], [10], [13], [38] and the newly developed unitary query adopted in the design of space-time coding for MIMO Backscatter RFID [14], [39]. In contrast to the diversity analysis in space-time coding where the message is coded over both space and time, here we focus on the transmit design against eavesdropping only in spatial domain and thus adopt conventional uniform query.



The achievable secrecy rate for a given secure transmission scheme determines the performance limit of PLS. Unfortunately, the exact expression of the secrecy rate here is difficult to obtain due to the non-Gaussian distribution of the combined signal and AN terms  $\mathbf{H}_{pr}\mathbf{F}_{tp}\mathbf{q}$  and  $\mathbf{H}_{pe}\mathbf{F}_{tp}\mathbf{q}$  received at the reader and the eavesdropper, respectively. However, following the similar method adopted in [23], we regard these terms as interference and obtain an approximation of the achievable secrecy rate given by [25]

$$C_s = [C_r - C_e]^+, \quad (7a)$$

$$C_r \approx \log_2 \det(\mathbf{I}_N + P_s \mathbf{H}_{pr} \mathbf{D}_{tp} \mathbf{D}_{tp}^H \mathbf{H}_{pr}^H \mathbf{R}_r^{-1}), \quad (7b)$$

$$C_e \approx \log_2 \det(\mathbf{I}_K + P_s \mathbf{H}_{pe} \mathbf{D}_{tp} \mathbf{D}_{tp}^H \mathbf{H}_{pe}^H \mathbf{R}_e^{-1}), \quad (7c)$$

where the covariance matrices of the interference and noise are given by

$$\mathbf{R}_r = \alpha \mathbf{H}_{pr} \mathbb{E}[\mathbf{F}_{tp} \mathbf{F}_{tp}^H] \mathbf{H}_{pr}^H + \beta \mathbf{H}_{tr} \mathbf{\Lambda}_z \mathbf{H}_{tr}^H + \sigma_r^2 \mathbf{I}_N, \quad (8a)$$

$$\mathbf{R}_e = \mathbf{H}_{pe} \mathbb{E}[\mathbf{F}_{tp} \mathbf{F}_{tp}^H] \mathbf{H}_{pe}^H + \mathbf{H}_{te} \mathbf{\Lambda}_z \mathbf{H}_{te}^H + \sigma_e^2 \mathbf{I}_K, \quad (8b)$$

with

$$\begin{aligned} \mathbb{E}[\mathbf{F}_{tp} \mathbf{F}_{tp}^H] &= \text{diag}\{\mathbb{E}[\mathbf{H}_{tp}^H \mathbf{z} \circ (\mathbf{z}^H \mathbf{H}_{tp})^T]\} \\ &= \mathbb{E}[\mathbf{H}_{tp}^H \mathbf{z} \mathbf{z}^H \mathbf{H}_{tp}] \circ \mathbf{I} \\ &= (\mathbf{H}_{tp}^H \mathbf{\Lambda}_z \mathbf{H}_{tp}) \circ \mathbf{I} \\ &= \sum_{i=1}^L (\mathbf{e}_i^T \mathbf{H}_{tp}^H \mathbf{\Lambda}_z \mathbf{H}_{tp} \mathbf{e}_i) (\mathbf{e}_i \mathbf{e}_i^T). \end{aligned}$$

From (7) and (8), to maximize the achievable secrecy rate in (7a) under the total power constraint in (3), the power allocation between the AN and the CW as well as the covariance matrix of AN  $\mathbf{\Lambda}_z$  needs to be carefully designed since the jamming signal from the reader degrades the performance of both the reader itself and the eavesdropper. The case where the tag has multiple antennas will be studied in the next two sections, while the scenario where a single antenna is employed at the tag will be investigated in Section V.

### III. MULTI-ANTENNA TAG

In this section, we consider the case where the tag equips with multiple antennas. The considered problems are first formulated as matrix optimization problems in Section III-A, and then the AO and SPCA methods are introduced to solve the SRM problem in Section III-B and Section III-C, respectively. The equivalence of the two methods in the considered problem will be illustrated in Section III-D.

#### A. Problem Formulation

To facilitate analysis, we first recast the secrecy rate in (7a) as

$$C_s(P_s, \mathbf{\Lambda}_z) = \ln \det(\mathbf{R}_r + P_s \mathbf{A}) + \ln \det(\mathbf{R}_e) - \ln \det(\mathbf{R}_r) - \ln \det(\mathbf{R}_e + P_s \mathbf{B}), \quad (9)$$

where  $\mathbf{A} \triangleq \mathbf{H}_{pr} \mathbf{D}_{tp} \mathbf{D}_{tp}^H \mathbf{H}_{pr}^H$  and  $\mathbf{B} \triangleq \mathbf{H}_{pe} \mathbf{D}_{tp} \mathbf{D}_{tp}^H \mathbf{H}_{pe}^H$ . Our aim is to maximize the achievable secrecy rate in (9) under

the total transmit power constraint in (3). Mathematically, this SRM problem can be formulated as follows:

$$\max_{P_s, \mathbf{\Lambda}_z} C_s(P_s, \mathbf{\Lambda}_z) \quad \text{s.t.} \quad (P_s, \mathbf{\Lambda}_z) \in \mathcal{C}, \quad (10)$$

where the feasible set is defined as

$$\mathcal{C} \triangleq \{(P_s, \mathbf{\Lambda}_z) \mid P_s + \text{Tr}(\mathbf{\Lambda}_z) \leq P, P_s \geq 0, \mathbf{\Lambda}_z \succeq \mathbf{0}\}. \quad (11)$$

As discussed in [29], [33], a simplified and special design of the general AN scheme in (10) is the so-called nullspace AN scheme where the transmitted AN lies in the nullspace of the legitimate user's channel. In our MIMO backscatter model, from (8a) we know that the reader receives two altered copies of its transmitted AN from the backscatter channel and the self-interference channel, respectively. When both the AN copies cannot be perfectly eliminated at the same time and the number of transmit antennas at the reader is adequate to perform the nullspace AN precoding, namely  $M > L$  or  $M > N$ , the AN transmitted by the reader can be designed to lie in the nullspace of the reader-tag channel  $\mathbf{H}_{tp}^H$  or the self-interference channel  $\mathbf{H}_{tr}$ , respectively. To be specific, we can construct the injected AN as  $\mathbf{z} = \mathbf{V}\mathbf{w}$ , and now we have

$$\mathbf{\Lambda}_z(\mathbf{W}) = \mathbf{V}\mathbf{W}\mathbf{V}^H, \quad (12)$$

where  $\mathbf{V}$  contains all the right singular vectors of  $\mathbf{H}_{tp}^H$  or  $\mathbf{H}_{tr}$  corresponding to zero singular values, and  $\mathbf{W} = \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$  is an  $(M-L) \times (M-L)$  or  $(M-N) \times (M-N)$  positive semidefinite matrix to be optimized, respectively. Mathematically, the nullspace SRM problem is formulated as follows:

$$\max_{P_s, \mathbf{W}} C_s(P_s, \mathbf{\Lambda}_z(\mathbf{W})) \quad \text{s.t.} \quad (P_s, \mathbf{W}) \in \mathcal{C}. \quad (13)$$

Since (13) is just a degenerate form of the SRM problem in (10), we will focus on solving (10) hereinafter.

The SRM problem in (10) is non-convex and difficult to tackle due to the non-concave property of the term  $-\ln \det(\cdot)$  in the objective function in (9). The AO and SPCA methods are the two methods widely exploited in tackling non-convex matrix optimization problems [30], [40], [41], and it will be interesting to see in the sequel that the two methods are actually equivalent under our SRM problem. Therefore, our approach is to reformulate the non-concave term to a concave one by exploiting the AO and SPCA methods. The two methods will be, respectively, introduced in the next two subsections.

#### B. AO Method for SRM

The main idea of the AO method is to exploit the coordinate-wise convexity property of the non-convex problem where optimization over two subsets of variables is non-convex, but optimization with respect to (w.r.t.) one while fixing the other is convex. To re-express the general SRM problem in (10) as a form that can be tackled by the AO method, we first introduce the following lemma.

**Lemma 1:** [42] Let  $\mathbf{X} \in \mathbb{C}^{N \times N}$  and  $\mathbf{X} \succ \mathbf{0}$ , then the function  $-\ln \det(\mathbf{X})$  can be equivalently rewritten by

importing an auxiliary variable  $\mathbf{S} \in \mathbb{C}^{N \times N}$  as

$$-\ln \det(\mathbf{X}) = \max_{\mathbf{S} \succeq \mathbf{0}} -\text{Tr}(\mathbf{S}\mathbf{X}) + \ln \det(\mathbf{S}) + N, \quad (14)$$

and the right-hand side of (14) has the optimal solution  $\mathbf{S}^* = \mathbf{X}^{-1}$  in a closed form.

From Lemma 1, one can easily see that the non-concave term can be changed to a linear (and thus concave) term w.r.t. the original optimization variable by adding an auxiliary variable. By applying Lemma 1 to the objective function in (9) via setting  $\mathbf{X}_0 = \mathbf{R}_r$  and  $\mathbf{X}_1 = \mathbf{R}_e + P_s \mathbf{B}$ , we have the following equivalent formulation of problem (10):

$$\begin{aligned} \max_{P_s, \Lambda_z, \mathbf{S}_0, \mathbf{S}_1} \quad & \ln \det(\mathbf{R}_r + P_s \mathbf{A}) + \ln \det(\mathbf{R}_e) \\ & - \text{Tr}(\mathbf{S}_0 \mathbf{R}_r) + \ln \det(\mathbf{S}_0) \\ & - \text{Tr}[\mathbf{S}_1 (\mathbf{R}_e + P_s \mathbf{B})] + \ln \det(\mathbf{S}_1) \\ \text{s.t.} \quad & (P_s, \Lambda_z) \in \mathcal{C}, \mathbf{S}_0 \succeq \mathbf{0}, \mathbf{S}_1 \succeq \mathbf{0}. \end{aligned} \quad (15)$$

Note that we have dropped the constant  $K + N$  in the objective of problem (15) for simplicity. The equivalent problem in (15) is non-convex w.r.t.  $(P_s, \Lambda_z, \mathbf{S}_0, \mathbf{S}_1)$ . However, it is not hard to see that problem (15) is convex w.r.t. either  $(P_s, \Lambda_z)$  or  $(\mathbf{S}_0, \mathbf{S}_1)$  while fixing the other. We can exploit this coordinate-wise convexity property to use the AO method to solve the problem. To be specific, let  $(P_s^n, \Lambda_z^n, \mathbf{S}_0^n, \mathbf{S}_1^n)$  denote the solution obtained at the  $n$ -th AO iteration. We iteratively use the values at the  $(n-1)$ -th iteration to obtain the ones at the  $n$ -th iteration by alternately solving the following two optimization problems for  $n = 1, 2, \dots$ ,

$$(\mathbf{S}_0^n, \mathbf{S}_1^n) = \arg \max_{\mathbf{S}_0, \mathbf{S}_1 \succeq \mathbf{0}} \ln \det(\mathbf{S}_0) - \text{Tr}(\mathbf{S}_0 \mathbf{R}_r^{n-1}) + \ln \det(\mathbf{S}_1) - \text{Tr}[\mathbf{S}_1 (\mathbf{R}_e^{n-1} + P_s^{n-1} \mathbf{B})], \quad (16a)$$

$$(P_s^n, \Lambda_z^n) = \arg \max_{(P_s, \Lambda_z) \in \mathcal{C}} \ln \det(\mathbf{R}_r + P_s \mathbf{A}) + \ln \det(\mathbf{R}_e) - \text{Tr}(\mathbf{S}_0^n \mathbf{R}_r) - \text{Tr}[\mathbf{S}_1^n (\mathbf{R}_e + P_s \mathbf{B})]. \quad (16b)$$

From Lemma 1, the optimal solution to problem (16a) takes a closed form and can be obtained by

$$\mathbf{S}_0^n = (\mathbf{R}_r^{n-1})^{-1}, \quad \mathbf{S}_1^n = (\mathbf{R}_e^{n-1} + P_s^{n-1} \mathbf{B})^{-1}. \quad (17)$$

Problem (16b) is convex, and thus can be numerically solved. The solution to our SRM problem can be obtained by iteratively calculating (17) and solving problem (16b) until the corresponding secrecy rate fulfills the given accuracy requirement.

As a basic result of AO, the method proposed above produces non-descending objective values. More specifically, we have  $C_s(P_s^0, \Lambda_z^0) \leq C_s(P_s^1, \Lambda_z^1) \leq \dots \leq C_s(P_s^n, \Lambda_z^n)$  [30]. In addition, we will show by Theorem 1 in Section III-D that the sequence  $\{P_s^n, \Lambda_z^n\}$  generated by the AO method converges to a Karush-Kuhn-Tucker (KKT) point of the original problem in (10).

### C. SPCA Method for SRM

As an alternative way, we can also use the SPCA method to solve the SRM problem in (10). The basic idea of the SPCA method is to approximate a non-convex problem by a sequence of convex problems. In each convex problem, every

non-convex constraint is replaced by an appropriate inner but convex one. Generally, the convergence rate of the SPCA method is fast. More details about SPCA can be found in [40], [41].

To apply the SPCA method, we first transform the non-concave terms in the objective function in (9) to the inner-approximated but concave ones. Note that the non-concave terms in the objective function are actually convex w.r.t. the optimization variable. Here the first-order Taylor's series approximation can be used as a global underestimator of the convex function  $-\ln \det(\mathbf{X})$  [43, p. 69]. More specifically, the approximation for the function  $-\ln \det(\mathbf{X})$  w.r.t.  $\mathbf{X} \succ \mathbf{0}$  around  $\mathbf{X}_0$  is given by

$$-\ln \det(\mathbf{X}) \geq -\ln \det(\mathbf{X}_0) - \text{Tr}[\mathbf{X}_0^{-1}(\mathbf{X} - \mathbf{X}_0)]. \quad (18)$$

From the right-hand side of (18), one can see that non-concave terms can be changed to linear (and thus concave) ones by exploiting this method.

By applying the approximation in (18) centering around the point  $(P_s^{n-1}, \Lambda_z^{n-1})$  to non-concave terms in the objective function in (9), we obtain (19) at the top of the next page where the superscript  $n-1$  refers to the optimal solution obtained at the  $(n-1)$ -th iteration. In each iteration we perform the approximation centering around the optimal solution obtained at the previous iteration. At the  $n$ -th iteration, the original non-convex SRM problem in (10) can be locally approximated by the following convex optimization problem for  $n = 1, 2, \dots$ ,

$$\begin{aligned} (P_s^n, \Lambda_z^n) = \arg \max_{(P_s, \Lambda_z) \in \mathcal{C}} \quad & f_0(P_s, \Lambda_z) \\ & - f_1(P_s, \Lambda_z, P_s^{n-1}, \Lambda_z^{n-1}) - f_2(P_s, \Lambda_z, P_s^{n-1}, \Lambda_z^{n-1}), \end{aligned} \quad (20)$$

where

$$f_0(P_s, \Lambda_z) \triangleq \ln \det(\mathbf{R}_r + P_s \mathbf{A}) + \ln \det(\mathbf{R}_e) \quad (21)$$

with  $f_1(P_s, \Lambda_z, P_s^{n-1}, \Lambda_z^{n-1})$  and  $f_2(P_s, \Lambda_z, P_s^{n-1}, \Lambda_z^{n-1})$  defined in (19). The solution to our SRM problem can be obtained by iteratively solving problem (20) until the corresponding secrecy rate fulfills the given accuracy requirement.

Like the AO method in the last subsection, the sequence of objective values produced by the SPCA method is non-descending. Moreover, we will show by Theorem 1 in the next subsection that the sequence  $\{P_s^n, \Lambda_z^n\}$  generated by the SPCA method converges to a KKT point of the original SRM problem in (10).

**Remark 1:** As seen in Section III-A, the nullspace SRM problem in (13) is just a degenerate form of the SRM problem in (10) when the nullspace AN constraint in (12) is imposed. Thus, once the general SRM problem in (10) is solved by the AO or SPCA method, the nullspace SRM problem in (13) can be easily solved in a similar way.

**Remark 2:** Generally, the AO and SPCA methods are two totally different methods and either the AO or SPCA method *individually* will give a solution. However, it is interesting to see that the two methods are actually *equivalent* for our SRM problem in the sense that the two methods can equivalently lead to the same optimization problem. We will analyze this equivalence in the next subsection.

$$\begin{aligned} \ln \det(\mathbf{R}_r) &\leq f_1(P_s, \mathbf{\Lambda}_z, P_s^{n-1}, \mathbf{\Lambda}_z^{n-1}) \triangleq \ln \det(\mathbf{R}_r^{n-1}) \\ &\quad + \text{Tr} \left\{ (\mathbf{R}_r^{n-1})^{-1} [\alpha \mathbf{H}_{pr} ((\mathbf{H}_{tp}^H (\mathbf{\Lambda}_z - \mathbf{\Lambda}_z^{n-1}) \mathbf{H}_{tp}) \circ \mathbf{I}) \mathbf{H}_{pr}^H + \beta \mathbf{H}_{tr} (\mathbf{\Lambda}_z - \mathbf{\Lambda}_z^{n-1}) \mathbf{H}_{tr}^H] \right\}, \end{aligned} \quad (19a)$$

$$\begin{aligned} \ln \det(\mathbf{R}_e + P_s \mathbf{B}) &\leq f_2(P_s, \mathbf{\Lambda}_z, P_s^{n-1}, \mathbf{\Lambda}_z^{n-1}) \triangleq \ln \det(\mathbf{R}_e^{n-1} + P_s^{n-1} \mathbf{B}) + \text{Tr} \{ (\mathbf{R}_e^{n-1} + P_s^{n-1} \mathbf{B})^{-1} \\ &\quad [\mathbf{H}_{pe} ((\mathbf{H}_{tp}^H (\mathbf{\Lambda}_z - \mathbf{\Lambda}_z^{n-1}) \mathbf{H}_{tp}) \circ \mathbf{I}) \mathbf{H}_{pe}^H + \mathbf{H}_{te} (\mathbf{\Lambda}_z - \mathbf{\Lambda}_z^{n-1}) \mathbf{H}_{te}^H + (P_s - P_s^{n-1}) \mathbf{B}] \}. \end{aligned} \quad (19b)$$

#### D. Equivalence, Convergence, and Complexity Analyses

As for the AO method, the equivalence can be verified by putting (17) in (16b), and then we obtain the following convex optimization problem at the  $n$ -th iteration:

$$(P_s^n, \mathbf{\Lambda}_z^n) = \arg \max_{(P_s, \mathbf{\Lambda}_z) \in \mathcal{C}} g(P_s, \mathbf{\Lambda}_z, P_s^{n-1}, \mathbf{\Lambda}_z^{n-1}), \quad (22)$$

where

$$\begin{aligned} g(P_s, \mathbf{\Lambda}_z, P_s^{n-1}, \mathbf{\Lambda}_z^{n-1}) &\triangleq f_0(P_s, \mathbf{\Lambda}_z) - \text{Tr}((\mathbf{R}_r^{n-1})^{-1} \mathbf{R}_r) \\ &\quad - \text{Tr}[(\mathbf{R}_e^{n-1} + P_s^{n-1} \mathbf{B})^{-1} (\mathbf{R}_e + P_s \mathbf{B})]. \end{aligned} \quad (23)$$

It is not hard to see that the objective function of problem (20) obtained by the SPCA method and (23) only differ in some added terms that are irrespective of our optimization variable  $(P_s, \mathbf{\Lambda}_z)$ , and thereby have no effect on the optimization result. This leads to the equivalence of the two methods for the considered SRM problem.

The main reasons for this equivalence are summarized as follows:

- 1) As for the SPCA method, the terms  $\mathbf{R}_r$  and  $\mathbf{R}_e + P_s \mathbf{B}$  in  $-\ln \det(\cdot)$  of the objective function in (9) are linear w.r.t. the optimization variable  $(P_s, \mathbf{\Lambda}_z)$ . This linear property makes the terms  $-\ln \det(\cdot)$  in the objective function convex, and thus the approximation of the first-order Taylor's series in (18) can be applicable. The choice of this approximation in the SPCA method makes the equivalence between problem (20) obtained by the SPCA method and problem (22) possible.
- 2) Concerning the AO method, Lemma 1 plays an important role in this equivalence. It should be noted that the specific way to apply the AO method actually depends largely on the form of the considered problem. In our case, it is the non-concave term  $-\ln \det(\cdot)$  that makes Lemma 1 applicable, and then the AO method can be employed to lead us to problem (22).
- 3) It can be observed that (14) in Lemma 1 of the AO method is actually closely related to (18) in the SPCA method. This is because (14) means that

$$\begin{aligned} -\ln \det(\mathbf{X}) &\geq -\text{Tr}(\mathbf{S}\mathbf{X}) + \ln \det(\mathbf{S}) + N, \\ &\quad \text{for any } \mathbf{X} \succ 0, \mathbf{S} \succeq 0 \\ \xrightarrow{\mathbf{S}=\mathbf{X}_0^{-1}} -\ln \det(\mathbf{X}) &\geq -\text{Tr}[\mathbf{X}_0^{-1}(\mathbf{X} - \mathbf{X}_0)] - \ln \det(\mathbf{X}_0), \\ &\quad \text{for any } \mathbf{X} \succ 0, \end{aligned} \quad (24)$$

which is exactly (18).

Since we have shown that both the AO and SPCA methods for our SRM problem are equivalent to iteratively solving the convex optimization problem in (22), the two methods actually

have the same convergence result and computational complexity. We first give the convergence result in the following theorem.

**Theorem 1:** Both the AO and SPCA methods produce non-descending achievable secrecy rates and converge to a KKT point of the original SRM problem in (10).

*Proof:* The proof is given in Appendix A. ■

At each AO or SPCA iteration, the convex optimization problem in (22) can be solved by using a general-purpose convex optimization toolbox, such as CVX [44], to obtain a numerical solution. This computational complexity can be approximated by the complexity of solving a standard semidefinite program (SDP) problem through the interior point method, though problem (22) is not a standard SDP problem. Problem (22) has  $M^2$  independent real and imaginary parts in the Hermitian matrix  $\mathbf{\Lambda}_z$ . Let  $J$  denote the total number of the AO or SPCA iteration. Then the complexity cost of the AO or SPCA method is at most  $O(JM^7)$  [45], while the cost reduces to at most  $O(J(M-L)^7)$  or  $O(J(M-N)^7)$  for the two nullspace SRM problems in (13). These computational complexity costs are usually much less when the modern SDP solver like SeDuMi [46] in CVX is employed.

#### IV. A FAST PG ALGORITHM FOR SRM WITH A MULTI-ANTENNA TAG

As we have indicated, the RFID system is typically resource-constrained compared with the conventional wireless communication system. Thus, it particularly requires low-complexity algorithms in practice. In this section, by exploiting the characteristic of the feasible set of the SRM problem in (10), we develop a fast and low-complexity algorithm based on projected gradient (PG) to replace the inefficient CVX while solving the convex problem in (22).

Let  $(P_s^{n,k}, \mathbf{\Lambda}_z^{n,k})$  denote the result obtained in the  $k$ -th inner PG iteration at the  $n$ -th outer equivalent AO or SPCA iteration. The general PG iteration is given by [47]

$$\begin{aligned} &(\bar{P}_s^{n,k+1}, \bar{\mathbf{\Lambda}}_z^{n,k+1}) \\ &= P_C(P_s^{n,k} + \mu_k \nabla_{P_s} g^{n,k}, \mathbf{\Lambda}_z^{n,k} + \mu_k \nabla_{\mathbf{\Lambda}_z} g^{n,k}), \quad (25a) \\ &(\bar{P}_s^{n,k+1}, \bar{\mathbf{\Lambda}}_z^{n,k+1}) \\ &= (P_s^{n,k}, \mathbf{\Lambda}_z^{n,k}) + \nu_k (\bar{P}_s^{n,k+1} - P_s^{n,k}, \bar{\mathbf{\Lambda}}_z^{n,k+1} - \mathbf{\Lambda}_z^{n,k}), \quad (25b) \end{aligned}$$

where  $\mu_k > 0$  and  $0 < \nu_k \leq 1$  are positive step sizes,  $P_C$  denotes the projection on the feasible set  $\mathcal{C}$  in (11), i.e.,

$$P_C(\tilde{P}_s, \tilde{\mathbf{\Lambda}}_z) \triangleq \arg \min_{(P_s, \mathbf{\Lambda}_z) \in \mathcal{C}} (P_s - \tilde{P}_s)^2 + \|\mathbf{\Lambda}_z - \tilde{\mathbf{\Lambda}}_z\|_F^2, \quad (26)$$

$$\begin{aligned} \nabla_{\Lambda_z} g^{n,k} = & \beta \mathbf{H}_{tr}^H [(\mathbf{F}^{n,k})^{-1} - \mathbf{S}_0^H] \mathbf{H}_{tr} + \mathbf{H}_{te}^H [(\mathbf{R}_e^{n,k})^{-1} - \mathbf{S}_1^H] \mathbf{H}_{te} \\ & + \sum_{i=1}^L \left\{ \alpha \text{Tr} [((\mathbf{F}^{n,k})^{-1} - \mathbf{S}_0^H) \mathbf{C}_i] + \text{Tr} [((\mathbf{R}_e^{n,k})^{-1} - \mathbf{S}_1^H) \mathbf{D}_i] \right\} \mathbf{E}_i, \end{aligned} \quad (27a)$$

$$\nabla_{P_s} g^{n,k} = \text{Tr}[(\mathbf{F}^{n,k})^{-1} \mathbf{A}] - \text{Tr}(\mathbf{S}_1^H \mathbf{B}). \quad (27b)$$

$$\mathbf{C}_i \triangleq \mathbf{H}_{pr} \mathbf{e}_i \mathbf{e}_i^T \mathbf{H}_{pr}^H, \quad \mathbf{D}_i \triangleq \mathbf{H}_{pe} \mathbf{e}_i \mathbf{e}_i^T \mathbf{H}_{pe}^H, \quad \mathbf{E}_i \triangleq \mathbf{H}_{tp} \mathbf{e}_i \mathbf{e}_i^T \mathbf{H}_{tp}^H, \quad \mathbf{F}^{n,k} \triangleq \mathbf{R}_r^{n,k} + P_s^{n,k} \mathbf{A}. \quad (28)$$

and  $(\nabla_{P_s} g^{n,k}, \nabla_{\Lambda_z} g^{n,k})$  denotes the gradient of the function  $g(P_s, \Lambda_z, P_s^{n-1}, \Lambda_z^{n-1})$  in (23) w.r.t.  $(P_s, \Lambda_z)$  at the point  $(P_s^{n,k}, \Lambda_z^{n,k})$ , which is shown in (27) at the top of the page where  $\mathbf{C}_i, \mathbf{D}_i, \mathbf{E}_i$ , and  $\mathbf{F}^{n,k}$  are defined in (28) with  $\mathbf{S}_0^H$  and  $\mathbf{S}_1^H$  defined in (17). To be specific,  $\nabla_{\Lambda_z} g$  here is actually the conjugate derivative of a real function  $g$  w.r.t. a Hermitian matrix, which falls into the field of generalized complex-valued matrix derivatives and follows from [48]. Note that once the initial value for the PG method  $(P_s^{n,0}, \Lambda_z^{n,0})$  is chosen to be feasible, i.e.  $(P_s^{n,0}, \Lambda_z^{n,0}) \in \mathcal{C}$ , it is clear that the sequence  $\{P_s^{n,k}, \Lambda_z^{n,k}\}$  generated by the PG method is feasible for any fixed  $n$  due to the projection operation in (25a) and the condition  $0 < \nu_k \leq 1$ . By exploiting the structure of the set  $\mathcal{C}$ , the projection  $P_{\mathcal{C}}$  in (26) can be formulated in a semi-closed form, which is shown in the following theorem.

**Theorem 2:** Let  $\tilde{\Lambda}_z = \mathbf{U} \text{diag}\{\tilde{\eta}\} \mathbf{U}^H$  be the eigenvalue decomposition of  $\tilde{\Lambda}_z$ . Then the optimal solution to problem (26) is given by

$$P_{\mathcal{C}}(\tilde{P}_s, \tilde{\Lambda}_z) = (P_s^*, \mathbf{U} \text{diag}\{\eta^*\} \mathbf{U}^H), \quad (29)$$

where  $P_s^*$  and  $\eta^*$  are unique and take the form

$$[P_s^*, \eta^{*T}]^T = \left[ [\tilde{P}_s, \tilde{\eta}^T]^T - \lambda^* \mathbf{1} \right]^+, \quad (30)$$

with  $\mathbf{1} \triangleq [1, 1, \dots, 1]^T$  and the water-filling level  $\lambda^*$  chosen as the minimum nonnegative value such that  $P_s^* + \eta^{*T} \mathbf{1} \leq P$ .

*Proof:* The proof is given in Appendix B. ■

We remark that the water-filling level  $\lambda^*$  in Theorem 2 can be efficiently obtained by some practical algorithms based on hypothesis testing [49]. As for the choosing of the step sizes  $\mu_k$  and  $\nu_k$  in the PG method, several strategies obeying the Armijo rule [47, Section 2.3.1] can be exploited. Here, we fix the second step size as  $\nu_k = 1$ , while the backtracking line search [43] is adopted to determine the first step size  $\mu_k$ . In this way, the iteration in (25) degenerates into

$$\begin{aligned} (P_s^{n,k+1}, \Lambda_z^{n,k+1}) \\ = P_{\mathcal{C}}(P_s^{n,k} + \mu_k \nabla_{P_s} g^{n,k}, \Lambda_z^{n,k} + \mu_k \nabla_{\Lambda_z} g^{n,k}). \end{aligned} \quad (31)$$

The iteration in (31) is guaranteed to converge to the global maximum for the convex optimization problem in (22) [50], and it achieves a good balance between the convergence rate and computational complexity [51]. The procedure of backtracking line search for choosing  $\mu_k$  is listed in Algorithm 1. The parameter  $\gamma \in (0, 1)$ , and typical algorithmic parameters are  $\mu_0 = 1$ ,  $\gamma = 0.5$ , and  $\delta = 0.1$ . Algorithm 1 is referred to as the Armijo search along the boundary of  $\mathcal{C}$  [47], [50].

---

#### Algorithm 1 Backtracking Line Search for Choosing $\mu_k$

---

**Input:**  $\mu = \mu_0$ ;

1: **while true do**

2:   Compute  $(P_s^{n,k+1}, \Lambda_z^{n,k+1})$  according to (31);

3:   **if**  $g^{n,k+1} > g^{n,k} + \delta \cdot \{\text{Tr}[(\nabla_{\Lambda_z} g^{n,k})^H (\Lambda_z^{n,k+1} - \Lambda_z^{n,k})] + \nabla_{P_s} g^{n,k} (P_s^{n,k+1} - P_s^{n,k})\}$  **then**

4:     **Break;**

5:   **end if**

6:    $\mu = \gamma \mu$ ;

7: **end while**

8: **return**  $\mu_k = \mu$ ;

---

We summarize our fast algorithm for SRM, combining the PG method for inner convex problem with the formerly proposed outer AO or SPCA iteration, in Algorithm 2, where  $C_s^n$  and  $g^{n,k}$  are used to denote  $C_s(P_s^n, \Lambda_z^n)$  and  $g(P_s^n, \Lambda_z^n, P_s^{n-1}, \Lambda_z^{n-1})$ , respectively, for notational convenience.

The main computational complexity of Algorithm 2 lies in the multiplication, inverse, and eigenvalue decomposition of a matrix. To facilitate the complexity comparison with CVX given in Section III-D, here we give the complexity cost of Algorithm 2 w.r.t.  $M$  only, which is  $O(JRM^3)$ , where  $J$  denotes the total iteration number of the outer AO or SPCA method as before and  $R$  represents the average iteration number of the inner PG method at each outer iteration. Recalling the computational complexity of CVX given in Section III-D, we see that the improvement in that of the fast PG algorithm is significant. This observation will also be verified by the simulations in Section VI.

Note that this fast PG algorithm can be also applied to solve the nullspace SRM problem in (13) after some modifications. From the chain rule of the gradient, the gradient of the function  $g(P_s, \Lambda_z(\mathbf{W}), P_s^{n-1}, \Lambda_z(\mathbf{W}^{n-1}))$  w.r.t.  $\mathbf{W}$  at the point  $\mathbf{W}^{n,k}$  is given by

$$\nabla_{\mathbf{W}} g^{n,k} = \mathbf{V}^H \nabla_{\Lambda_z} g^{n,k} \mathbf{V}, \quad (32)$$

where  $\mathbf{V}$  is defined in Section III-A. With the optimization variable changed to  $\mathbf{W}$  and the gradient changed to (32), we can still apply Algorithm 2 to efficiently solve the nullspace SRM problem in (13).

## V. SINGLE-ANTENNA TAG

In the previous sections, we have solved the SRM problem with a multi-antenna tag. In real applications, due to the



---

**Algorithm 2** Fast PG Algorithm for SRM
 

---

**Input:**  $P, n = 1, (P_s^0, \Lambda_z^0) \in \mathcal{C}, \epsilon_1 > 0, \epsilon_2 > 0;$

- 1: **while**  $|(C_s^n - C_s^{n-1})/C_s^{n-1}| > \epsilon_1$  **do**
- 2:    $k = 0, (P_s^{n,0}, \Lambda_z^{n,0}) = (P_s^{n-1}, \Lambda_z^{n-1});$
- 3:   **while**  $|(g^{n,k} - g^{n,k-1})/g^{n,k-1}| > \epsilon_2$  **do**
- 4:     Compute  $\nabla_{\Lambda_z} g^{n,k}$  according to (27);
- 5:     Compute the step size  $\mu_k$  according to Algorithm 1;
- 6:     Calculate  $(\tilde{P}_s, \tilde{\Lambda}_z) = (P_s^{n,k} + \mu_k \nabla_{P_s} g^{n,k}, \Lambda_z^{n,k} + \mu_k \nabla_{\Lambda_z} g^{n,k});$
- 7:     Calculate  $(P_s^{n,k+1}, \Lambda_z^{n,k+1}) = P_C(\tilde{P}_s, \tilde{\Lambda}_z)$  according to (29)-(30);
- 8:      $k = k + 1;$
- 9:   **end while**
- 10:    $(P_s^n, \Lambda_z^n) = (P_s^{n,k}, \Lambda_z^{n,k});$
- 11:    $n = n + 1;$
- 12: **end while**
- 13: **return**  $(P_s^*, \Lambda_z^*) = (P_s^n, \Lambda_z^n);$

---

resource and cost constrained property of the RFID network, currently a single antenna is usually used at the tag in the market [12]. Thus, it is necessary to consider security issues under the scenario where the tag has a single antenna, while the reader and the eavesdropper have multiple antennas. It should be noted that previously proposed methods can still be exploited to obtain a *local optimal* solution for this scenario. In this section, we focus on finding a low-complexity algorithm which yields the *global optimal* solution to the SRM problem with a single-antenna tag under some practical assumptions.

When the tag employs a single antenna, all the channels form/to the tag reduce to vectors and we redefine  $D_{tp} \triangleq \sqrt{1/M} \mathbf{h}_{tp}^H \mathbf{1}_M$ . To facilitate analysis and obtain the traceable optimal solution to the SRM problem with a single-antenna tag, here we make the following two assumptions:

- 1) The eavesdropper is not aware of the noise injection scheme and thereby simply adopts maximum ratio combining (MRC) to deal with the received signal. Note that when the noise injection scheme is known by the eavesdropper, it may adaptively apply the minimum mean square error (MMSE) receiver to mitigate the jamming from the reader. The SRM problem under this scenario can be similarly tackled by the methods used in the multi-antenna tag case.
- 2) The reader transmits the AN signal in the nullspace of its self-interference channel, which is a practical assumption mainly in that the reader can equip with only one more antenna for transmitting compared with for receiving. It should be noted that the mathematical model under this assumption is similar to the one under the assumption that the reader can perfectly cancel the AN received from the self-interference channel, i.e.,  $\beta = 0$ . Thus, for notational simplicity we only consider the latter assumed situation in this section.

Under the above two assumptions, the achievable rates in (7b)

and (7c) now change to

$$\begin{aligned} C_r^{\text{MMSE,ZF}} &= \log_2 (1 + P_s |d_{tp}|^2 \mathbf{h}_{pr}^H (\alpha \mathbf{h}_{pr} \mathbf{h}_{pr}^H (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \sigma_r^2 \mathbf{I})^{-1} \mathbf{h}_{pr}) \\ &\stackrel{(a)}{=} \log_2 \left( 1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pr}\|^2}{\alpha \|\mathbf{h}_{pr}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \sigma_r^2} \right) \end{aligned}$$

and

$$\begin{aligned} C_e^{\text{MRC}} &= \log_2 \left( 1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pe}\|^2}{\|\mathbf{h}_{pe}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \frac{\mathbf{h}_{pe}^H \mathbf{H}_{te} \Lambda_z \mathbf{H}_{te}^H \mathbf{h}_{pe}}{\|\mathbf{h}_{pe}\|^2} + \sigma_e^2} \right), \end{aligned}$$

respectively, where (a) follows from the matrix inverse lemma. The SRM problem with a single-antenna tag now becomes

$$\begin{aligned} \max_{P_s, \Lambda_z} \quad & \frac{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pr}\|^2}{\alpha \|\mathbf{h}_{pr}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \sigma_r^2}}{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pe}\|^2}{\|\mathbf{h}_{pe}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \frac{\mathbf{h}_{pe}^H \mathbf{H}_{te} \Lambda_z \mathbf{H}_{te}^H \mathbf{h}_{pe}}{\|\mathbf{h}_{pe}\|^2} + \sigma_e^2}} \\ \text{s.t.} \quad & P_s + \text{Tr}(\Lambda_z) \leq P, \quad P_s \geq 0, \quad \Lambda_z \succeq \mathbf{0}. \end{aligned} \quad (33)$$

In the following, we will show that although problem (33) is still non-convex, its optimal solution is traceable. The basic idea to solve problem (33) is to reduce the original problem to a single-argument optimization problem, and then the optimal solution can be efficiently obtained by one-dimensional search. Before proceeding, we first give the following lemma about the rank property of the optimal AN covariance  $\Lambda_z^*$  for problem (33).

**Lemma 2:** The optimal AN covariance  $\Lambda_z^*$  for problem (33) is rank-one.

*Proof:* To show the optimal  $\Lambda_z^*$  is rank-one for problem (33), we first let  $\|\mathbf{h}_{pe}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \mathbf{h}_{pe}^H \mathbf{H}_{te} \Lambda_z \mathbf{H}_{te}^H \mathbf{h}_{pe} / \|\mathbf{h}_{pe}\|^2 = s$  be fixed and the optimal  $\Lambda_z^*$  must satisfy

$$\begin{aligned} \Lambda_z^* &= \arg \min_{\Lambda_z} \mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp} \\ \text{s.t.} \quad & \|\mathbf{h}_{pe}\|^2 (\mathbf{h}_{tp}^H \Lambda_z \mathbf{h}_{tp}) + \mathbf{h}_{pe}^H \mathbf{H}_{te} \Lambda_z \mathbf{H}_{te}^H \mathbf{h}_{pe} / \|\mathbf{h}_{pe}\|^2 = s, \\ & \text{Tr}\{\Lambda_z\} \leq P, \quad \Lambda_z \succeq \mathbf{0}. \end{aligned} \quad (34)$$

To see more clearly, the above problem can be recast as

$$\begin{aligned} \Lambda_z^* &= \arg \min_{\Lambda_z} \text{Tr}\{\mathbf{C}_1 \Lambda_z\} \\ \text{s.t.} \quad & \text{Tr}\{\mathbf{C}_2 \Lambda_z\} = s, \quad \text{Tr}\{\Lambda_z\} \leq P, \quad \Lambda_z \succeq \mathbf{0}, \end{aligned} \quad (35)$$

where  $\mathbf{C}_1 \triangleq \mathbf{h}_{tp} \mathbf{h}_{tp}^H$  and  $\mathbf{C}_2 \triangleq \|\mathbf{h}_{pe}\|^2 \mathbf{h}_{tp} \mathbf{h}_{tp}^H + \mathbf{H}_{te}^H \mathbf{h}_{pe} \mathbf{h}_{pe}^H \mathbf{H}_{te} / \|\mathbf{h}_{pe}\|^2$ . Problem (35) takes a semidefinite relaxation (SDR) form of a complex-valued homogeneous quadratically constrained quadratic program (QCQP) with two constraints. According to the conclusion in [52], the SDR is tight and the solution of problem (35) is rank-one. This completes the proof. ■

In addition, we remark that the optimal solution to problem (33) must satisfy the total power constraint with equality. This can be shown by contradiction. Suppose that the optimal solution to problem (33) is  $(P_s^*, \Lambda_z^*)$  with  $P_s^* + \text{Tr}\{\Lambda_z^*\} < P$ , then we can construct a new feasible solution  $(P_s^*, \Lambda_z^*)$  such that  $P_s^* + \text{Tr}\{\Lambda_z^*\} = P$  where  $\tilde{\Lambda}_z = \Lambda_z^* + \mathbf{r} \mathbf{r}^H$ ,  $\mathbf{h}_{tp}^H \mathbf{r} = 0$ , and



$$\max_{P_s, \mathbf{v}} \frac{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pr}\|^2}{\alpha \|\mathbf{h}_{pr}\|^2 (P - P_s) (\mathbf{v}^H \mathbf{h}_{tp} \mathbf{h}_{tp}^H \mathbf{v}) + \sigma_r^2}}{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pe}\|^2}{\|\mathbf{h}_{pe}\|^2 (P - P_s) (\mathbf{v}^H \mathbf{h}_{tp} \mathbf{h}_{tp}^H \mathbf{v}) + (P - P_s) \mathbf{v}^H \mathbf{H}_{te}^H \mathbf{h}_{pe} \mathbf{h}_{pe}^H \mathbf{H}_{te} \mathbf{v} / \|\mathbf{h}_{pe}\|^2 + \sigma_e^2}}} \quad \text{s.t. } \|\mathbf{v}\| = 1, 0 \leq P_s \leq P. \quad (36)$$

$$\max_{P_s, t} y(P_s, t) \triangleq \frac{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pr}\|^2}{\alpha \|\mathbf{h}_{pr}\|^2 \|\mathbf{h}_{tp}\|^2 (P - P_s) t + \sigma_r^2}}{1 + \frac{P_s |d_{tp}|^2 \|\mathbf{h}_{pe}\|^2}{\|\mathbf{h}_{pe}\|^2 \|\mathbf{h}_{tp}\|^2 (P - P_s) t + \|\mathbf{H}_{te}^H \mathbf{h}_{pe}\|^2 (P - P_s) r(t) / \|\mathbf{h}_{pe}\|^2 + \sigma_e^2}}} \quad \text{s.t. } 0 \leq t \leq 1, 0 \leq P_s \leq P. \quad (38)$$

$\mathbf{h}_{pe}^H \mathbf{H}_{te} \mathbf{r} \neq 0$ . It can be easily verified that  $(P_s^*, \bar{\Lambda}_z)$  yields a larger objective value, which is a contradictory.

From the above discussions about the properties of the optimal solution to problem (33), the AN covariance matrix can be expressed as  $\Lambda_z = (P - P_s) \mathbf{v} \mathbf{v}^H$  where  $\|\mathbf{v}\| = 1$ . We can further recast problem (33) as problem (36) shown at the top of the page. Problem (36) is still difficult to handle, to facilitate the further analysis we first consider the optimization of  $\mathbf{v}$  in problem (36). Let  $\mathbf{v}^H \mathbf{d}_1 \mathbf{d}_1^H \mathbf{v} = t$ ,  $0 \leq t \leq 1$  where  $\mathbf{d}_1 \triangleq \mathbf{h}_{tp} / \|\mathbf{h}_{tp}\|$ . By considering the following subproblem

$$r(t) \triangleq \max_{\mathbf{v}} \mathbf{v}^H \mathbf{d}_2 \mathbf{d}_2^H \mathbf{v} \quad \text{s.t. } \mathbf{v}^H \mathbf{d}_1 \mathbf{d}_1^H \mathbf{v} = t, \|\mathbf{v}\| = 1, \quad (37)$$

where  $\mathbf{d}_2 \triangleq \mathbf{H}_{te}^H \mathbf{h}_{pe} / \|\mathbf{H}_{te}^H \mathbf{h}_{pe}\|$ , then problem (36) can be reduced to problem (38) shown at the top of the page. The following lemma gives the closed-form solution to the subproblem in (37).

**Lemma 3:** [34] Let  $\phi \in (-\pi, \pi]$  be the argument of  $\mathbf{d}_2^H \mathbf{d}_1$ ,  $\kappa = |\mathbf{d}_1^H \mathbf{d}_2| \neq 1$ . Then the optimal solution to problem (37) and the corresponding objective function value are given by

$$\mathbf{v}^*(t) = \left( \kappa \sqrt{\frac{1-t}{1-\kappa^2}} - \sqrt{t} \right) e^{i(\pi-\phi)} \mathbf{d}_1 + \sqrt{\frac{1-t}{1-\kappa^2}} \mathbf{d}_2, \quad (39)$$

$$r(t) = 1 - \left( \kappa \sqrt{1-t} - \sqrt{(1-\kappa^2)t} \right)^2. \quad (40)$$

Now our aim reduces to solve the two-argument optimization problem in (38). To solve problem (38), our method is to first find the optimal  $P_s^*(t)$  for any given  $t$  and then perform the one-dimensional search w.r.t.  $t$ . To facilitate analysis, for any given  $t$  we recast the objective function in problem (38) w.r.t.  $P_s$  as

$$y^t(P_s) = \frac{1 + \frac{a P_s}{1 + b P_s}}{1 + \frac{c P_s}{1 + d P_s}}, \quad (41)$$

where

$$\begin{aligned} a &\triangleq |d_{tp}|^2 \|\mathbf{h}_{pr}\|^2 / (\sigma_r^2 + P l_1), \quad b \triangleq -l_1 / (\sigma_r^2 + P l_1), \\ c &\triangleq |d_{tp}|^2 \|\mathbf{h}_{pe}\|^2 / (\sigma_e^2 + P l_2), \quad d \triangleq -l_2 / (\sigma_e^2 + P l_2), \\ l_1 &\triangleq \alpha \|\mathbf{h}_{pr}\|^2 \|\mathbf{h}_{tp}\|^2 t, \\ l_2 &\triangleq \|\mathbf{h}_{pe}\|^2 \|\mathbf{h}_{tp}\|^2 t + \|\mathbf{H}_{te}^H \mathbf{h}_{pe}\|^2 r(t) / \|\mathbf{h}_{pe}\|^2. \end{aligned}$$

Let the first order derivative of  $y^t(P_s)$  in (41) be zero, we obtain

$$(ad^2 + acd - abc - b^2c)P_s^2 + 2(ad - bc)P_s + (a - c) = 0. \quad (42)$$

The solution to the above quadratic equation is given by

$$P_{s,1(2)}^t = \frac{ad - bc \pm \sqrt{ac(b-d)(a+b-c-d)}}{b^2c + a(bc - d(c+d))}, \quad (43)$$

and the optimal power allocated to the CW signal at the reader for any given  $t$  becomes

$$P_s^*(t) = \arg \max_{P_s} y(P_s, t), \quad P_s \in \{P_{s,1}^t, P_{s,2}^t, P\} \cap [0, P], \quad (44)$$

which can be easily computed. Substituting (44) into problem (38) yields a single-argument optimization problem, which can be handled by searching  $t$  in the interval  $[0, 1]$ . Once we have obtained the optimal  $t^*$ , the optimal power allocated to the CW signal and the optimal AN covariance matrix are given by  $P_s^* = P_s^*(t^*)$  and  $\Lambda_z^* = (P - P_s^*) \mathbf{v}^*(t^*) \mathbf{v}^{*H}(t^*)$ , respectively.

As in Section III-A, here we also consider a suboptimal nullspace AN scheme. More specifically, we can restrict the transmitted AN from the reader to lie in the nullspace of the reader-tag channel  $\mathbf{h}_{tp}$ . Under this condition, we directly have  $t = 0$  and the only remaining thing is to obtain  $P_s^*(0)$  by solving the low-complexity problem in (44). Thus, the computational complexity can be vastly reduced. Note that when the total available power or the number of antennas at the transmitter of the reader is large, this nullspace AN constraint incurs a loss of only one degree of freedom which is negligible compared with the large number of antennas. So from this view, this scheme is practical and beneficial for resource-constrained RFID devices and it achieves a good trade-off between secrecy performance and computational complexity. This observation will be verified by the simulation in the next section.

## VI. SIMULATION RESULTS

This section presents some numerical results to evaluate the secrecy rate performance of the proposed noise-injection precoding schemes as well as their computational efficiency. In the simulations, the self-interference channel at the reader is generated as  $\mathbf{H}_{tr} = \tilde{\mathbf{H}}_{tr}$ , and the other channels are assumed to undergo a path loss combined with a small-scale fading, namely  $\mathbf{H}_k = d_k^{-\gamma/2} \tilde{\mathbf{H}}_k$ ,  $k \in \{tp, te, pe, pr\}$ , where  $d_k$  is the distance between two nodes,  $\gamma$  is the path loss exponent, and each element of  $\tilde{\mathbf{H}}_j$ ,  $j \in \{tr, tp, te, pe, pr\}$ , is an independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and unit variance. Note that the statistic distribution of the self-interference channel at the reader has not been well understood yet [53]. Thus, for simplicity we adopt this distribution here as in [54].

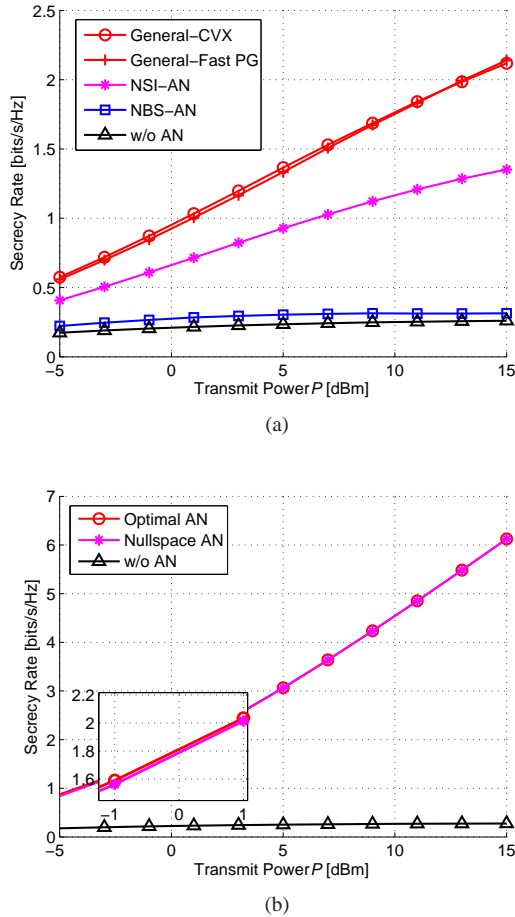


Fig. 2. The secrecy rates  $C_s$  achieved by different schemes versus the total transmit power of the reader  $P$  under (a) multi-antenna and (b) single-antenna tag cases. For both the two cases, the attenuation factors of the backscattered AN are the same  $\alpha = 0.6$ . For the multi-antenna tag case, the attenuation factor of the self-interference  $\beta = 0.3$ , and  $\beta = 0$  for the single-antenna tag case.

The simulation settings are as follows, unless otherwise specified: The antenna numbers at the receiver and the transmitter of the reader, the tag, and the eavesdropper are  $N = 2$ ,  $M = 3$ ,  $L = 2$ , and  $K = 3$ , respectively. The typical transmit power at the reader  $P = 10$  dBm, and the AWGN power at the reader and the eavesdropper  $\sigma_e^2 = \sigma_r^2 = -20$  dBm. The path loss exponent is set as  $\gamma = 2$ , and we set typical distances between two nodes as  $d_k = 2$  m,  $k \in \{tp, te, pe, pr\}$ . We initialize our algorithms with the initial power allocation  $\rho^0 = 1$ ,  $P_s^0 = \rho^0 P$ ,  $\Lambda_z^0 = (1 - \rho^0)(P/M)\mathbf{I}$  and set with the termination parameters  $\epsilon_1 = 10^{-3}$  and  $\epsilon_2 = 10^{-5}$ . In addition, to obtain a larger secrecy rate in the general AN design, we use the solution obtained by the nullspace AN scheme as the initial parameter. Note that under the above antenna number setting the reader can perform two nullspace AN schemes, namely, the no backscattered AN (NBS-AN) scheme and the no self-interference AN (NSI-AN) scheme where the transmitted AN lies in the nullspace of the reader-tag channel and the self-interference channel, respectively. All results to be shown are averaged over 1000 randomly generated channel realizations.

Fig. 2 shows the secrecy rates achieved by different schemes versus the transmit power  $P$  under both the multi-antenna tag

TABLE I  
AVERAGE RUNNING TIME (IN SECS.) VERSUS TRANSMIT POWER

Method		Transmit Power (dBm)				
		-3	1	5	9	13
Multi-Antenna Tag Case	General-CVX	11.8927	12.1476	12.3213	12.5497	12.4153
	<b>General-Fast PG</b>	<b>0.2266</b>	<b>0.2725</b>	<b>0.3118</b>	<b>0.3787</b>	<b>0.4902</b>
Single-Antenna Tag Case	Optimal AN	0.0164	0.0164	0.0164	0.0164	0.0164
	<b>Nullspace AN</b>	<b>0.0006</b>	<b>0.0006</b>	<b>0.0006</b>	<b>0.0006</b>	<b>0.0006</b>

case (cf. Fig. 2(a)) and the single-antenna tag case (cf. Fig. 2(b)). In the multi-antenna tag case, we evaluate the performance of the general AN design obtained by the proposed fast PG algorithm in Algorithm 2 (labeled as “General-Fast PG”), and compare it with the general AN design obtained by CVX (labeled as “General-CVX”), the two nullspace AN schemes, and the scheme without AN. It can be observed from Fig. 2(a) that the advantage of the proposed noise-injection scheme is significant compared with the scheme without AN especially when  $P$  is large. As shown in Fig. 2(a), the general AN design outperforms the two nullspace AN schemes as it is free from the nullspace AN constraint. One can also see that the proposed fast PG algorithm achieves almost the same secrecy rate as CVX does. In addition, to illustrate the relative computing efficiency of the proposed algorithms for SRM, we present the corresponding average running time in Table I<sup>4</sup>. One can see that the fast PG algorithm is much faster than CVX. In the single-antenna tag case, we compare the performance of the optimal AN design with the nullspace AN precoding. It can be observed from Fig. 2(b) that the secrecy rate achieved by the nullspace AN precoding is very close to the optimal one. Moreover, through Table I we see that the nullspace AN precoding enjoys a much lower computational complexity compared with the optimal AN design. The nullspace AN precoding here achieves a good trade-off between secrecy performance and computational complexity. These low-complexity algorithms are especially beneficial to resource-constrained RFID devices.

Fig. 3(a) plots the secrecy rates achieved by different schemes versus the attenuation factor of the backscattered AN  $\alpha$  under the multi-antenna tag case. From the figure, we see that the secrecy rates decreases as  $\alpha$  increases. Note that the secrecy rate achieved by the NBS-AN scheme remains constant. This is because the injected noise is fully nulled out at the tag in this scheme. From Fig. 3(a), the secrecy rate achieved by the general AN design drops down significantly and approaches to the one obtained by the NBS-AN scheme when  $\alpha$  becomes larger. This is because the backscattered AN received by the reader cannot be well attenuated at this time. Another interesting observation is that the performance of the NSI-AN scheme is close to the general AN design when  $\alpha$  is small, and the performance gap of the two schemes becomes larger as  $\alpha$  increases. This is because the NSI-AN scheme is close to the optimal scheme only when the self-interference dominates, namely  $\alpha$  is small.

<sup>4</sup> The average running time listed in Table I is obtained by a desktop with MATLAB as the simulation tool. This result is only for the purpose of relative comparison between different algorithms, and the measurement of the practical running time on a typical RFID device is out of the scope of this paper.

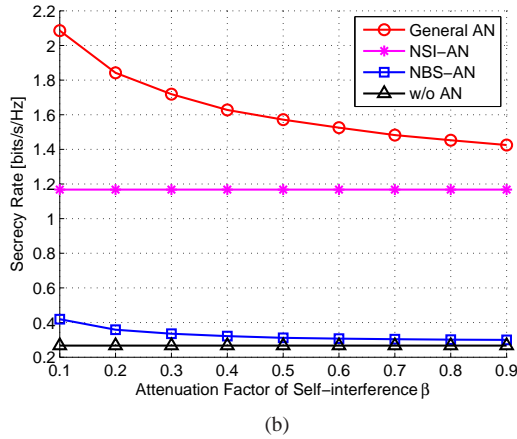
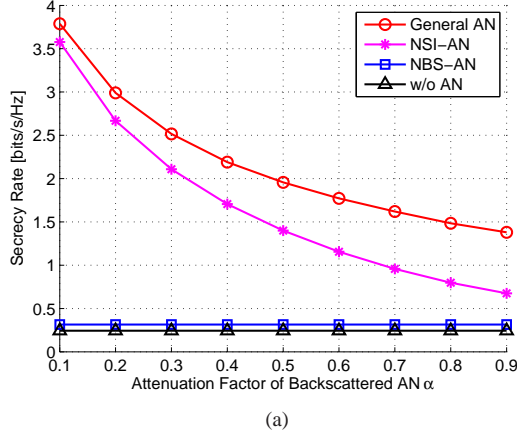


Fig. 3. (a) The secrecy rates achieved by different schemes versus the attenuation factor of the backscattered AN  $\alpha$  where the attenuation factor of the self-interference is fixed as  $\beta = 0.3$ , and (b) the secrecy rates achieved by different schemes versus the attenuation factor of the self-interference  $\beta$  where the attenuation factor of the backscattered AN is fixed as  $\alpha = 0.6$ . Both figures are under the multi-antenna tag case.

Fig. 3(b) depicts the secrecy rates achieved by different schemes against the attenuation factor of the self-interference  $\beta$  under the multi-antenna tag case. We can clearly see that the secrecy rates decrease with an increase in  $\beta$ . Note that the secrecy rate achieved by the NSI-AN scheme remains constant, because the self-interference is fully nulled out at the reader in this scheme. It can be seen from Fig. 3 that no matter how  $\alpha$  or  $\beta$  changes the NSI-AN scheme is always superior to the NBS-AN scheme. This is because the received backscattered AN at the reader goes through both the reader-tag and the tag-reader channels and thus experience a double path loss compared with the received AN from the self-interference channel. Hence, the received AN due to self-interference generally dominates in the received signal at the reader, and thus the secrecy rate achieved by the NSI-AN scheme is much closer to that achieved by the general AN design. Similarly, this nullspace scheme can serve as a low-complexity method which achieves a good trade-off between secrecy performance and computational complexity in the RFID system.

Fig. 4 shows the secrecy rates achieved by different schemes when we increase the number of the reader's transmit antennas  $M$  (cf. Fig. 4(a)) or the eavesdropper's antennas  $K$  (cf. Fig.

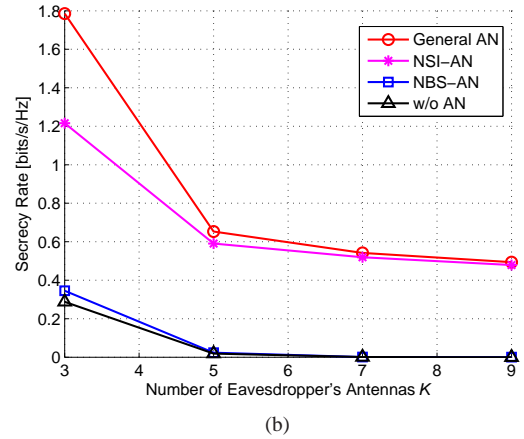
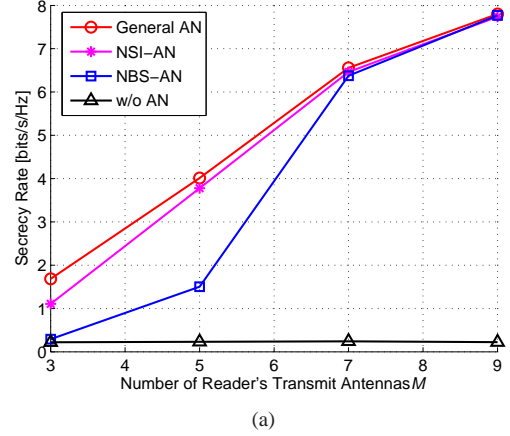


Fig. 4. (a) The secrecy rates achieved by different schemes versus the number of the reader's transmit antennas  $M$ , and (b) the secrecy rates achieved by different schemes versus the number of the eavesdropper's antennas  $K$ . The attenuation factors of the backscattered AN and self-interference are  $\alpha = 0.6$  and  $\beta = 0.3$ , respectively. Both figures are under the multi-antenna tag case.

4(b)) under the multi-antenna tag case. Again, we can see that the superiority of noise-injection schemes on SRM is significant. Note that from Fig. 4(b), the NBS-AN scheme and the scheme without AN cannot even achieve a positive secrecy rate when the number of the eavesdropper's antennas is larger than six. As shown in Fig. 4(a), the two nullspace AN schemes achieve almost the same secrecy rate as the general AN design does, when the number of the reader's transmit antennas satisfies  $M > 7$ . This is not surprising because a large number of transmit antennas brings abundant spatial degrees of freedom and the performance loss incurred by the nullspace AN constraint is negligible. Under this situation, it is beneficial for the reader to perform the nullspace AN schemes to reduce the computational complexity and obtain the near-optimal performance.

We then study the impact of the eavesdropper's location on the secrecy rate performance. For simplicity, we assume that the reader, the tag, and the eavesdropper are located on a straight line in this order. Fig. 5 shows the secrecy rates achieved by different schemes versus the tag-eavesdropper distance  $d_{pe}$  ranging from 0.8 m to 2 m under the multi-antenna tag case, where the reader-tag distance  $d_{tp}$  is set to either 2 m (indicated by the solid line) or 2.5 m (indicated

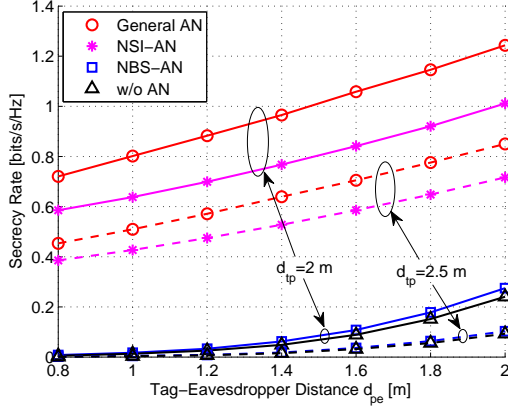


Fig. 5. The secrecy rates achieved by different schemes versus the tag-eavesdropper distance  $d_{pe}$  under the multi-antenna tag case. The reader-tag distance  $d_{tp}$  is set to either 2 m (indicated by the solid line) or 2.5 m (indicated by the dashed line). The reader, the tag, and the eavesdropper are located on a straight line in this order. The attenuation factors of the backscattered AN and self-interference are  $\alpha = 0.6$  and  $\beta = 0.3$ , respectively.

by the dashed line). From Fig. 5, we see that the secrecy rate strongly depends on the distances between the nodes due to the power-law decay of the path loss. Indeed, the secrecy rate under the small reader-tag distance is larger than that under the large one. Moreover, the secrecy rate increases significantly as the tag-eavesdropper distance increases. In particular, when  $d_{tp} = 2$  m and the eavesdropper is very close to the tag (e.g.  $d_{pe} = 0.8$  m), from Fig. 5 the general AN design can achieve a positive secrecy rate larger than 0.7 bits/s/Hz, while the scheme without AN cannot even achieve a positive secrecy rate. This implies that the proposed noise-injection scheme and the optimization of the AN covariance matrix can give the secrecy rate a sharp boost when the eavesdropper is very close to the tag.

## VII. CONCLUSION

In this paper, we have studied security issues in a MIMO RFID backscatter system from the perspective of PLS. First, we have proposed a noise-injection precoding scheme. Then, we have changed the non-convex SRM problem to a sequence of convex ones by exploiting the AO and SPCA methods, respectively. Interestingly, we have shown a fact that the two methods are actually equivalent for our SRM problem. Moreover, to facilitate the implementation for resource-constrained RFID devices, a fast algorithm based on the PG method has been proposed. As a complement, we have studied the single-antenna tag case and derived an algorithm yielding the global optimal solution. Numerical results show the superior secrecy rate performance of the proposed noise-injection precoding schemes and the low computational complexity of the proposed algorithms. Furthermore, the proposed nullspace schemes can achieve a good balance between secrecy performance and computational complexity for the resource-constrained RFID system.

## APPENDIX A PROOF OF THEOREM 1

Here we only show the convergence of the SPCA method for our SRM problem, and the same convergence result holds for the AO method due to the equivalence of the two methods in Section III-D. We divide the proof into two steps: First, we show that the SPCA method produces non-descending achievable secrecy rates and converges to a limit point; Second, we further show that the method converges to a KKT point of the SRM problem in (10).

At the  $n$ -th iteration of the SPCA method, let  $(P_s^n, \Lambda_z^n)$  be the optimal solution to problem (20), and it is straightforward to see that the optimal solution  $(P_s^{n-1}, \Lambda_z^{n-1})$  at the  $(n-1)$ -th iteration is only a feasible solution at the  $n$ -th iteration of the SPCA method. Thus, we have

$$\begin{aligned} & f_0(P_s^n, \Lambda_z^n) - f_1(P_s^n, \Lambda_z^n, P_s^{n-1}, \Lambda_z^{n-1}) \\ & \quad - f_2(P_s^n, \Lambda_z^n, P_s^{n-1}, \Lambda_z^{n-1}) \\ & \geq f_0(P_s^{n-1}, \Lambda_z^{n-1}) - f_1(P_s^{n-1}, \Lambda_z^{n-1}, P_s^{n-1}, \Lambda_z^{n-1}) \\ & \quad - f_2(P_s^{n-1}, \Lambda_z^{n-1}, P_s^{n-1}, \Lambda_z^{n-1}) \\ & = C_s(P_s^{n-1}, \Lambda_z^{n-1}). \end{aligned} \quad (45)$$

On the other hand, from (19) we have

$$\begin{aligned} & f_0(P_s^n, \Lambda_z^n) - f_1(P_s^n, \Lambda_z^n, P_s^{n-1}, \Lambda_z^{n-1}) \\ & \quad - f_2(P_s^n, \Lambda_z^n, P_s^{n-1}, \Lambda_z^{n-1}) \leq C_s(P_s^n, \Lambda_z^n). \end{aligned} \quad (46)$$

Combining (45) with (46) leads to  $C_s(P_s^n, \Lambda_z^n) \geq C_s(P_s^{n-1}, \Lambda_z^{n-1})$ , which completes the proof for the non-descending property of the achievable secrecy rates produced by the SPCA method. Note that the achievable secrecy rate  $C_s$  is up-bounded for any given transmit power  $P$ . Thereby we conclude that the proposed SPCA method converges to a limit point.

The KKT-point convergence result can be straightforwardly verified from [40, Theorem 1]. From [40, Step 1], we know that the first-order Taylor's series approximation in (18) satisfies the constraints for ensuring the SPCA method. Then from [40, Theorem 1], the convergence to a KKT point of the original problem is guaranteed. This completes the proof.

## APPENDIX B PROOF OF THEOREM 2

To fulfill the proof, we first illustrate the original projection problem in (26) can be reduced to a simplex projection problem given by

$$\begin{aligned} (P_s^*, \boldsymbol{\eta}^*) &= \arg \min_{P_s, \boldsymbol{\eta}} (P_s - \tilde{P}_s)^2 + \|\boldsymbol{\eta} - \tilde{\boldsymbol{\eta}}\|^2 \\ \text{s.t. } & P_s \geq 0, \boldsymbol{\eta} \geq \mathbf{0}, P_s + \boldsymbol{\eta}^T \mathbf{1} \leq P. \end{aligned} \quad (47)$$

By unitary invariance of the Frobenius norm, problem (26) is equivalent to

$$\begin{aligned} & \min_{(P_s, \Lambda_z) \in \mathcal{C}} (P_s - \tilde{P}_s)^2 + \|\Lambda_z - \mathbf{U} \text{diag}\{\tilde{\boldsymbol{\eta}}\} \mathbf{U}^H\|_F^2 \\ & \iff \min_{(P_s, \Lambda_z) \in \mathcal{C}} (P_s - \tilde{P}_s)^2 + \|\mathbf{U}^H \Lambda_z \mathbf{U} - \text{diag}\{\tilde{\boldsymbol{\eta}}\}\|_F^2 \\ & \iff \min_{(P_s, \Lambda_z) \in \mathcal{C}} (P_s - \tilde{P}_s)^2 + \|\hat{\Lambda}_z - \text{diag}\{\tilde{\boldsymbol{\eta}}\}\|_F^2, \end{aligned} \quad (48)$$



where  $\hat{\Lambda}_z \triangleq \mathbf{U}^H \Lambda_z \mathbf{U}$ . It can be easily seen by contradiction that the optimal solution  $\hat{\Lambda}_z^*$  to problem (48) must take the form of a diagonal matrix. Let  $\hat{\Lambda}_z = \text{diag}\{\eta\}$ , and then problem (48) can be equivalently changed to the simplex projection problem in (47). From  $\text{diag}\{\eta^*\} = \mathbf{U}^H \Lambda_z^* \mathbf{U}$ , we obtain the structure of the optimal solution as shown in (29).

As for the simplex projection problem in (47), it is well studied in [55] and its optimal solution is given by the water-filling solution in (30). This completes the proof.

## REFERENCES

- [1] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, Oct. 2005.
- [2] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jun. 2006.
- [3] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*. Newnes, 2007.
- [4] C. Boyer and S. Roy, "Backscatter communication and RFID: Coding, energy, and MIMO analysis," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 770–785, Mar. 2014.
- [5] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-Fi backscatter: Internet connectivity for RF-powered devices," in *Proc. Sigcomm*, Chicago, IL, Aug. 2014.
- [6] N. Pillin, N. Joehl, C. Dehollain, and M. J. Declercq, "High data rate RFID tag/reader architecture using wireless voltage regulation," in *Proc. IEEE Int. Conf. RFID*, Las Vegas, NV, Apr. 2008, pp. 141–149.
- [7] M. Gossar, M. Gebhart, P. Soser, and H. Witschnig, "Development of an evaluation reader for 13.56 MHz RFID systems providing very high data rates up to 6.78 Mbit/s," in *Proc. 11th Int. Conf. Telecommun. (ConTEL)*, Graz, Austria, Jun. 2011, pp. 31–38.
- [8] N. C. Karmakar, *Handbook of Smart Antennas for RFID Systems*. New Jersey: Wiley, 2010.
- [9] F. Zheng and T. Kaiser, *Digital Signal Processing for RFID*. Wiley, 2016.
- [10] M. A. Ingram, M. F. Demirkol, and D. Kim, "Transmit diversity and spatial multiplexing for RF links using modulated backscatter," in *Symp. Int. Signals, Systems, and Electronics*, Tokyo, Japan, Jul. 2001.
- [11] J. D. Griffin and G. D. Durgin, "Gains for RF tags using multiple antennas," *IEEE Trans. Antennas Propag.*, vol. 56, no. 2, pp. 563–570, Feb. 2008.
- [12] F. Zheng and T. Kaiser, "On the transmit signal design at the reader for RFID MIMO systems," in *Proc. 4th Int. EURASIP Workshop on RFID Technol. (EURASIP RFID)*, Torino, Italy, Sep. 2012, pp. 59–64.
- [13] C. Boyer and S. Roy, "Space time coding for backscatter RFID," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2272–2280, May 2013.
- [14] C. He, Z. J. Wang, and V. C. M. Leung, "Unitary query for the  $M \times L \times N$  MIMO backscatter RFID channel," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2613–2625, May 2015.
- [15] M. B. Akbar, M. M. Morys, C. R. Valenta, and G. D. Durgin, "Range improvement of backscatter radio systems at 5.8 GHz using tags with multiple antennas," in *Proc. 2012 IEEE Int. Symp. on Antennas and Propagation*, Chicago, IL, Jul. 2012, pp. 1–2.
- [16] E. Denicke, M. Henning, H. Rabe, and B. Geck, "The application of multipoint theory for MIMO RFID backscatter channel measurements," in *European Microwave Conf.*, Amsterdam, Netherlands, Oct. 2012, pp. 522–525.
- [17] M. S. Trotter, C. R. Valenta, G. A. Koo, B. R. Marshall, and G. D. Durgin, "Multi-antenna techniques for enabling passive RFID tags and sensors at microwave frequencies," in *2012 IEEE Int. Conf. on RFID*, Orlando, FL, Apr. 2012, pp. 1–7.
- [18] S. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security Privacy*, vol. 3, no. 3, pp. 34–43, May 2005.
- [19] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.
- [20] H. Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 337–340, Oct. 2007.
- [21] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Des. Test. Comput.*, vol. 24, no. 6, pp. 522–533, Jun. 2007.
- [22] E. Vahedi, R. K. Ward, and I. F. Blake, "Security analysis and complexity comparison of some recent lightweight RFID protocols," *Lecture Notes in Computer Science*, vol. 6694, no. 11, pp. 92–99, Jun. 2011.
- [23] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.
- [24] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [25] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [26] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.
- [28] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Dallas, TX, Sep. 2005, pp. 1906–1910.
- [29] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eaves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
- [30] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
- [31] H.-M. Wang, T.-X. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.
- [32] H.-M. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.
- [33] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.
- [34] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
- [35] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
- [36] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.
- [37] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Asilomar Conf. Sign. Syst. Comput.*, Pacific Grove, CA, Nov. 2011, pp. 265–269.
- [38] C. He and Z. J. Wang, "SER of orthogonal space-time block codes over rician and nakagami- $m$  RF backscattering channels," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 654–663, Feb. 2014.
- [39] C. He, Z. J. Wang, C. Miao, and V. C. M. Leung, "Block-level unitary query: Enabling orthogonal-like space-time code with query diversity for MIMO backscatter RFID," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1937–1949, Mar. 2016.
- [40] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, Jul./Aug. 1978.
- [41] A. Beck, A. Ben-Tal, and L. Tetrushvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Global Optim.*, vol. 47, no. 1, pp. 29–51, May 2010.
- [42] J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On robust weighted-sum rate maximization in MIMO interference networks," in *Proc. IEEE Int. Conf. Communications (ICC)*, Kyoto, Japan, Jun. 2011.
- [43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [44] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," <http://cvxr.com/cvx>, Apr. 2011.
- [45] Y. Ye, *Interior Point Algorithms: Theory and Analysis*. New York: Wiley, 1997.
- [46] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optim. Methods Softw.*, vol. 11–12, pp. 625–653, Mar. 1999.

- [47] D. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1999.
- [48] A. Hjørungnes, *Complex-Valued Matrix Derivatives*. Cambridge University Press, 2011.
- [49] D. P. Palomar and J. R. Fonollosa, "Practical algorithms for a family of waterfilling solutions," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 686–695, Feb. 2005.
- [50] A. N. Iusem, "On the convergence properties of the projected gradient method for convex optimization," *Comput. Appl. Math.*, vol. 22, no. 1, pp. 37–52, Jun. 2003.
- [51] X. Jiang, W.-J. Zeng, A. Yasotharan, H. C. So, and T. Kirubarajan, "Quadratically constrained minimum dispersion beamforming via gradient projection," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 192–205, Jan. 2015.
- [52] Z. Q. Luo, W. K. Ma, A. M. C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [53] K. Alexandris, A. Balatsoukas-Stimming, and A. Burg, "Measurement-based characterization of residual self-interference on a full-duplex MIMO testbed," in *Proc. IEEE Sens. Array Multichannel Signal Processing Workshop*, A Coruna, Spain, Jun. 2014, pp. 329–332.
- [54] G. Zheng, "Joint beamforming optimization and power control for full-duplex MIMO two-way relay channel," *IEEE Trans. Signal Process.*, vol. 63, no. 3, pp. 555–566, Feb. 2015.
- [55] D. P. Palomar, "Convex primal decomposition for multicarrier linear MIMO transceivers," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4661–4674, Dec. 2005.